REMARKS

The Examiner is thanked for the performance of a thorough search.

STATUS OF CLAIMS

Claims 2-5, 8, 10, 12, 14, 16, 19-26, 28, 30, 32, have been cancelled.

Claims 1, 9, 11, 13, 15, 18, 27, 29, 31, and 34-36 have been amended.

Claims 37-72 have been added.

No claims have been withdrawn.

Claims 1, 6-7, 9, 11, 13, 15, 17-18, 27, 29, 31, and 33-72 are currently pending in the application.

INFORMATION DISCLOSURE STATEMENTS & FORM 1449'S

The Applicant thanks the Examiner for returning with the Office Action the initialed and dated Form 1449's from the Information Disclosure Statements filed on December 6, 2001 and February 25, 2002.

However, the Office Action also included a third initialed Form 1449 that was received by the Office on December 28, 1001 for application Serial No. 09/560,695, which is not the present application being examined, nor is application Serial No. 09/560,695 being handled by the Applicant's representative.

The Applicant is calling this situation to the Examiner's attention so that the third Form 1449 can be sent to the proper recipient for application Serial No. 09/560,695.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claims 15-16 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite. Claims 1-16 and 27-36 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent Application Publication Number US 2003/0031316 A1 of Langston et al. (" *Langston* ") in view of U.S. Patent Application Publication Number US 2002/0039418 A1 of Dror et al. (" *Dror* "). Claims 17-26 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Langston* in view of *Dror* and in further view of "Modulo Reduction in Residue Number Systems" by Posch et al. (" *Posch*"). The rejections are respectfully traversed.

RESPONSE TO REJECTIONS NOT BASED ON THE PRIOR ART

Claims 15-16 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Office Action states that "Claims 15 and 16 are indefinite because, in conjunction with the independent claim 1, the claim language 'intermediate result' is based on the modular operation (Claim 1 Line 11-12) where modular operation is again based on the intermediate result (Claim 15 Line 1-3 and Claim 16 Line 1-4) and thereby constitutes an indefinite feedback function because it is not clearly and uniquely pointed out what constitutes the 'intermediate result' as any of other parameters does in the claim limitations."

Claim 1 features two "determining" steps, one for "determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant" and the other for "determining...a final result...based on at least Montgomery's method for the modular operation, the intermediate result, and the second operand." As originally written, Claim 15 features that the "modular operation is a modular exponentiation that is based on at least the second operand, a second constant, the modulus, a negative multiplicative inverse of the modulus, and the intermediate result" and then recites specific steps for determining the final result. Thus, it can be observed that Claim 15 is referring to the determination of the final result in Claim 1, but not the determination of the intermediate result of Claim 1. However, as written, Claim 15 modifies the "modular operation" that is featured in Claim 1 in determining both the intermediate result and the final result, and hence the Office Action observes that this appears to create "an indefinite feedback function," which was not intended.

As amended above, Claim 15 specifies that "the modular operation <u>for determining the final result</u> is a modular exponentiation that is based on at least...the intermediate result" to clarify that the modular operation for determining the final result is a modular exponentiation that is based on the intermediate result. While the modular expression for determining the intermediate result in Claim 1 may or may not be a modular exponentiation, the amendment to Claim 15 makes clear that the additional features of Claim 15 do not involve the "determining an intermediate result" step of Claim 1 and do not modify the "modular operation" for determining the intermediate result in Claim 1. Thus, the apparent "indefinite feedback

function" noted in the Office Action is removed as a result of the amendment to Claim 15. Similar clarifications to Claims 9, 11, and 13 have been included in the amendments above.

The Applicant respectfully submits that the amendment to Claim 15 traverses the rejection of Claim 15 under 35 U.S.C. § 112, second paragraph, and that because Claim 16 has been cancelled, the rejection of Claim 16 under 35 U.S.C. § 112, second paragraph is rendered moot.

RESPONSE TO REJECTIONS BASED ON THE PRIOR ART

Claims 1-16 and 27-36 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Langston* in view of *Dror*. Claims 17-26 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Langston* in view of *Dror* and in further view of *Posch*. The rejections are respectfully traversed.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

"A method for encryption and decryption of electronic messages based on an encryption protocol, the method comprising the computer-implemented steps of:

receiving a first electronic message that is encrypted according to the encryption protocol;

generating at least one part of a second electronic message, based on at least the first electronic message, a modular operation that is based on **two applications of Montgomery's method**, a first operand, a second operand, and a modulus, and wherein the step of generating the second electronic message includes the computer-implemented steps of:

generating a first constant based on the modulus;

in a first application of Montgomery's method, determining an ***intermediate result*** based on at least Montgomery's method for the modular operation, the first operand, and the first constant; and

in a second application of Montgomery's method, determining and storing in memory a ***final result*** that comprises the at least one part of the second electronic message, based on at least Montgomery's method for the modular operation, the ***intermediate result***, and the second operand." (Emphasis added.)

Thus, Claim 1 features "**two applications of Montgomery's method.**" Specifically, Claim 1 features "**in a first application of Montgomery's method**, determining an ***intermediate result***..." and "**in a second application of Montgomery's method**, determining a ***final result***...based on at least...the ***intermediate result***." For example, in the embodiment depicted by FIG. 1 of the application, a first pass that includes the first application of Montgomery's method is performed in block 130 to determine an intermediate result based on the first operand, the pre-computed constant, and Montgomery's method for modular multiplication. Then in block 140, a second pass that includes the second application of Montgomery's method is performed to determine the final result based on the intermediate result, the second operand, and Montgomery's method for modular multiplication.

As discussed in the Background section of the application, a single pass or application of Montgomery's method for modular multiplication is implemented through three expressions. (Application, page 2, lines 20-22.) Note that both operands in the modular multiplication, X and Y, are used in this typical formulation of Montgomery's method, as can be seen in the first of the three expressions.

However, unlike the typical application of a single pass of Montgomery's method, in block 130, the first application of Montgomery's method is used to determine the intermediate result (S) based on the first operand (X) and the pre-computed constant (R) using a modified set of the three expressions for Montgomery's method for modular multiplication. (Application, page 12, lines 6-10.) In this first application of Montgomery's method of block 130, only the first operand in the modular multiplication, X, is used as an input to the first pass and the second operand, Y, is not used as an input.

Next in block 140, the second application of Montgomery's method is used to determine the final result (F) based on the second operand (Y) and the intermediate result (S) using yet another modified set of three expression for Montgomery's method for modular multiplication. (Application, page 12, lines 14-16.) In this second application of

Montgomery's method, only the second operand, Y, is used as in input in the second pass and the first operand, X, is not used as an input. The two applications of Montgomery's method as depicted in blocks 130 and 140 are "tied" together by using the result of the first application of Montgomery's method, the intermediate result (S), as one of the inputs for the second application of Montgomery's method to then determine the final result (F).

This approach -- using two passes or applications of Montgomery's method in which each application of Montgomery's method uses one of the two operands, and in which the result of the first application of Montgomery's method is used as an input to the second application of Montgomery's method -- is a fundamental difference between the approach of Claim 1 and the typical approach based on Montgomery's method in which both operands are used as input to a single application of Montgomery's method.

(2) INTRODUCTORY DISCUSSION OF *LANGSTON, DROR, AND POSCH*

In contrast to the approach of Claim 1, *Langston* discloses a full-adder post processor for modulo arithmetic. (Abstract.) The approach of *Langston* is directed to a hardware implementation in the form of an improved post processor for high-speed modulo reduction and addition, such as the full-adder post processor 104 of Figure 2 and the post processor 600 of Figure 6. (*Langston*, paragraph [0010].) *Langston* discloses that exponentiator 602 can support Montgomery multiplication and exponentiation, including the use of a plurality of carry save adders that can be operated in a pipelined manner to perform Montgomery calculations through the use of partial products. (*Langston*, paragraph [0500].) *Langston* only discloses the typical single application of Montgomery's method, and nowhere in *Langston* is there any disclosure of the use of two applications of Montgomery's method in which the result of the first application is used as input to the second application.

In contrast to the approach of Claim 1, *Dror* discloses an extension of a serial/parallel Montgomery modular multiplication method with simultaneous reduction. (Abstract.) *Dror* discusses the use of Montgomery's modular reduction method for use with Montgomery arithmetic on polynomial based numbers. (*Dror*, paragraphs [0276], [0278].) *Dror* then provides an example of the "conventional Montgomery method" for modular multiplication of the operands "A" and "B." (*Dror*, paragraphs [0311-0312].) Dror then uses Montgomery's interleaved reduction to perform multiplication operations with shorter operands, registers, and hardware multipliers to allow for implementations in devices with relatively fewer logic

gates. (*Dror*, paragraph [0332].) As with *Langston*, *Dror* only discloses the conventional single application of Montgomery's method, and nowhere in *Dror* is there any disclosure of the use of two applications of Montgomery's method in which the result of the first application is used as input to the second application.

Finally, in contrast to the approach of Claim 1, *Posch* discloses an approach for using residue number systems for modulo reduction. (Abstract.) Specifically, Posch describes residue number systems (RNS) as applied to modular multiplication (see section "II. Elements of Fast Reduction" beginning on page 449) and then applies the residue number system approach for Montgomery's method (see section "IV. Montgomery's Reduction in RNS" beginning on page 451). However, as with *Langston* and *Dror*, *Posch* only discloses the typical single application of Montgomery's method, and nowhere in *Posch* is there any disclosure of the use of two applications of Montgomery's method in which the result of the first application is used as input to the second application.

(3) THE OFFICE ACTION'S CITATIONS FROM *LANGSTON* AND *DROR*

Although Claim 1 features "a modular operation that is based on two applications of Montgomery's method," the Office Action fails to cite any portion of any reference as disclosing this feature of Claim 1. Specifically, the Office Action cites a portion of *Langston* as allegedly disclosing "generating at least one part of a second electronic message" and then recites the balance of the text of Claim 1 following this portion of this step, namely "based on at least the first electronic message, a modular operation that is based on two applications of Montgomery's method, a first operand, a second operand, and a modulus, and wherein the step of generating the second electronic message includes the computer-implemented steps of:..." However, the Office Action fails to provide any citation for the balance of the features of this generating step, particularly the feature "a modular operation that is based on **two applications of Montgomery's method**..." as recited in Claim 1.

In the rejection of Claim 1, the Office Action states that "Langston teaches determining an intermediate result (Langston: see for example, Claim 5)." However, Claim 5 in *Langston* is: "The cipher processing system of claim 4 wherein the intermediate result corresponds to the partial product." The "intermediate result" referred to in Claim 5 is recited in Claim 1 of *Langston* in the following limitation: "an exponentiator operable to perform modulo exponentiation comprising reducing the size of an intermediate result at least once

during modulo exponentiation computations..." (Emphasis added.) This means that the intermediate result being referred to in Claims 1 and 5 of *Langston* is an intermediate result reached ***during*** a single application of modulo exponentiation, such as in the typical single application of Montgomery's method upon which the techniques of *Langston* are based.

The "partial product" referred to in Claim 5 is recited in Claim 4 of *Langston* in the following limitation: "the operands from the exponentiator comprise carry data and sum data corresponding to a partial product." In *Langston*, the partial products are use by exponentiator 602 that uses "a plurality of carry save adders operating in a pipelined manner to perform the Montgomery calculations by calculating partial products." (*Langston*, [0050].) This means that the Montgomery calculations are implemented by *Dror* through the calculation of partial products within the application of Montgomery's method. Therefore, as with the "intermediate result," the partial product of Claim 5 of *Langston* is part of a single application of Montgomery's method.

Because both the "intermediate result" of Claims 1 and 5 and the "partial product" of Claims 4 and 5 of *Langston* refer to a single application of Montgomery's method, neither is in any way related to the "intermediate result" of Claim 1 of the application, little less the features of Claim 1 of "in a first application of Montgomery's method, determining an intermediate result..." and then "in a second application of Montgomery's method, determining a final result...based at least on...the intermediate result..."

While both *Langston* and Claim 1 of the present application use the phrase "intermediate result," a careful reading of *Langston* and Claim 1 shows that the phrase "intermediate result" has fundamentally different meanings in each. In *Langston*, "intermediate result" refers to a result that is reached during a single application of Montgomery's method that ultimately produces the desired final result. However, in Claim 1, "intermediate result" refers to the output from one application of Montgomery's method. The "intermediate result" is then used as the input to a second application of Montgomery's method to determine the desired "final result." In Claim 1 of the present application, the phrase "intermediate result" is used to indicate that a single application of Montgomery's method does not produce the desired final result, so as to distinguish the output of the first application of Montgomery's method (e.g., the "intermediate result) from the output of the second application of Montgomery's method (e.g., the "final result"). In contrast to Claim 1,

the "intermediate result" of *Langston* is the result of some, but not all, the calculations in a single application of Montgomery's method.

The Office Action then states that "Langston does not disclose expressly determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant," which appears to indicate that the Office Action has correctly understood that *Langston* discloses only a single application of Montgomery's method. However, then the Office Action states that "Dror teaches determining an intermediate result based on at least Montgomery's method for the modular operation, the first operand, and the first constant (Dror: see for example, Paragraph [0312] – [0326])."

In *Dror*, paragraphs [0312] through [0316] merely recite a single application of Montgomery's method for modular multiplication of the operands "A" and "B" through the five steps enumerated therein. Paragraphs [0317] through [0326] simply derive an expression (shown in paragraph [0326]) for the pre-computed constant "J" that must be determined in order to use Montgomery's method. Specifically, paragraph [0311] that notes that "J" must be precomputed according to the expression derived for "J" as shown in paragraph [0326] so that J can be used during Montgomery's method in the calculation according to the expression given in paragraph [0313]. Therefore, nothing in paragraphs [0312] through [0326] of *Dror* discloses anything about "in a first application of Montgomery's method, determining an intermediate result..." and then "in a second application of Montgomery's method, determining a final result...based on at least...the intermediate result..." as featured in Claim 1.

Finally, the Office Action states that it "would have been obvious...to combine the teach of Dror within the system of Langston because Dror teaches using Montgomery reduction with partial products to perform an efficient multiplication operations so that shorter operands, registers, and hardware multipliers are needed (Dror: see for example, Paragraph [0332])." However, paragraph [0332] in *Dror* states "Using Montgomery's interleaved reduction as described in P1, it is possible to perform the multiplication operations with shorter operands, registers, and hardware multipliers; enable the implementation of an electronic device with relatively few logic gates."

Thus, *Dror* says nothing about the use of partial products, little less anything about an intermediate result that is determined based on a first application of Montgomery's method

and that the intermediate result is used in a second application of Montgomery's method to determine a final result, as featured in Claim 1. Furthermore, paragraph [0332] only provides a motivation to combine the teachings of *Dror* with those of reference P1 (which is a prior patent of *Dror*, see paragraph [0002]), and there is nothing in paragraph [0332] that would motivate one to combine the teachings of *Dror* and *Langston*.

In considering the Office Action's rejection of Claim 1 as a whole, it appears to the Applicant that the Office Action is asserting that because *Langston* discloses applying Montgomery's method and that *Dror* also discloses applying Montgomery's method, that the two can then be combined to reach the approach of Claim 1 of the present application. The Office Action's rationale appears to be that because *Langston* can be considered to be one application of Montgomery's method and that *Dror* can be considered to be a second application of Montgomery's method, then *Langston* in combination with *Dror* discloses the "dual applications of Montgomery's method" as featured in Claim 1.

However, as explained above, each of *Langston* and *Dror* disclose only a single application of Montgomery's method. Furthermore, the approaches of *Langston* and *Dror* each begin with the same modular multiplication of two operands according to Montgomery's method to reach the same final result, albeit by using different hardware implementations. There is nothing in either of *Langston* or *Dror* that discloses or suggests anything about multiple applications of Montgomery's method, little less that a first application based on a first operand is used to determine an intermediate result, which is then used with a second operand in a second application of Montgomery's method to determine a final result, as featured in Claim 1. The references fail to suggest the particular combination recited in Claim 1.

Finally, although the Office Action does not rely upon *Posch* in the rejection of Claim 1, the Applicant notes that *Posch*, similar to *Langston* and *Dror*, discloses a single application of Montgomery's method, and therefore that Posch also fails to disclose "two applications of Montgomery's method" as featured in Claim 1.

(5) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *LANGSTON, DROR, AND POSCH*

Because *Langston*, *Dror*, and *Posch*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious "a modular operation that is based on **two applications of Montgomery's method**," "**in a first application of Montgomery's method**,

determining an ***intermediate result***...based on the first operand...," and "**in a second application of Montgomery's method**, determining...a ***final result***...based on at least... the ***intermediate result*** and the second operand," the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

C. CLAIMS 34-36

Claims 34-36 contain features that are similar to those described above with respect to Claim 1. In particular, Claims 34-36 all feature "a modular operation that is based on **two applications of Montgomery's method**," which is the same as in Claim 1. Also, Claims 34 and 36 both feature "**in a first application of Montgomery's method**, determining an ***intermediate result***...based on the first operand..." and "**in a second application of Montgomery's method**, determining...a ***final result***...based on at least... the ***intermediate result*** and the second operand," which is the same as in Claim 1. Finally, Claim 35 features "means for determining, **in a first application of Montgomery's method**, an ***intermediate result***...based on the first operand...," and "means for determining, **in a second application of Montgomery's method**,...a ***final result***...based on at least... the ***intermediate result*** and the second operand," which is similar to Claim 1. Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 34-36 are allowable over the art of record and are in condition for allowance.

D. CLAIMS 6-7, 9, 11, 13, 15, 17-18, 27, 29, 31, 33, AND 37-72

Claims 6-7, 9, 11, 13, 15, 17-18, 27, 29, 31, and 33 are dependent upon Claim 1, Claims 37-48 are dependent upon Claim 36, Claims 49-60 are dependent upon Claim 34, and Claims 61-72 are dependent upon Claim 35, and thus include each and every feature of the corresponding independent claims. Therefore, it is respectfully submitted that Claims 6-7, 9, 11, 13, 15, 17-18, 27, 29, 31, 33, and 37-72 are allowable for the reasons given above with respect to Claims 1 and 34-36.

In addition, each of Claims 6-7, 9, 11, 13, 15, 17-18, 27, 29, 31, 33, and 37-72 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive

resolution of this case a separate discussion of those limitations is not included at this time except for Claims 6-7, 37-38, 49-50, and 61-62, which are addressed below.

Claims 6, 37, 49, and 61 each feature "selecting a second constant (W) such that W≥ 4M" based on "the modulus (M)." The Office Action states that "Langston...teaches the step of...selecting a second constant (W) such that W≥4M...(Langston: see for example, claim 15: Montgomery constant as taught by Langston corresponds to W^2, where $W=r^{(n+8)}$)." However, Claim 15 in Langston is: "The cipher processing system of claim 12 wherein the Montgomery constant correspond to the value $r^{2(n+8)}$modN, where r is a number, N is the modulus, and n is the bit size of the modulus." While Claim 15 states that "r is a number," paragraph [0050] in *Langston* states that the "value of r is selected as an integer multiple of base two (e.g., 2^{16}) so that the value of $r^{2(n+8)}$ can be represented in binary form by a single one most significant bit following by many zeros..."

Thus, the value of "W" based on the Office Action's citation in *Langston* is that "W" is a function of a number "r" that is an integer multiple of base two and "n" that is the bit size of the modulus. However, Claims 6, 37, 49, and 61 feature selecting "W" so that "W≥4M," which means that "W" merely has a value of greater than or equal to four times the modulus (M). The Office Action's rejection based on *Langston* disclosing that "W" is based on an integer multiple of two and the bit size of the modulus says nothing about the value of "W", little less that "W" is selected to have a value of greater than or equal to four times the value of the modulus, as featured in Claims 6, 37, 49, and 61. The Applicants are unable to deduce any rationale that the Office Action might be relying upon for the assertion that the cited portion of Langston or any other portion of Langston discloses selecting "W" so that "W≥4M," as featured in Claims 6, 37, 49, and 61.

Because *Langston* fails to disclose, teach, suggest, or in any way render obvious "selecting a second constant (W) such that W≥ 4M" based on "the modulus (M)," the Applicant respectfully submits that, for at least the reasons stated above, Claims 6, 37, 49, and 61 are allowable over the art of record and is in condition for allowance.

Claims 7, 38, 50, and 62 each feature "the second constant (W) is not a power of two." The Office Action states that *Langston* teaches that "the second constant (W) is not a power of two (Langston: see for example, claim 15; r can be any number)." However, contrary to the assertion of the Office Action, Claim 15 does not disclose that "r" can be ***any*** number.

Rather, as noted above, Claim 15 states that "r is ***a*** number," and paragraph [0050] in *Langston* explains that the "value of r is selected as an ***integer multiple of base two*** (e.g., 2^{16}) so that the value of $r^{2(n+8)}$ can be represented in binary form by a single one most significant bit following by many zeros..." (Emphasis added.) Thus, the approach of *Langston* relies upon "r" being an integer multiple of base two, which means that the value of "r" must be a power of two.

Therefore, based on the Office Action equating $W=r^{(n+8)}$, the disclosure in *Langston* that "r" must be a power of two, and that as discussed above, *Langston* states that "n" is the bit size of the modulus, which means that "n" is an integer value, the value of "W" is also a power of two. Thus, the disclosure of *Langston* clearly and unambiguously contradicts the feature of Claims 7, 38, 50, and 62 that "the second constant (W) is not a power of two."

Because *Langston* not only fails to disclose, teach, suggest, or in any way render obvious "selecting a second constant (W) such that $W \geq 4M$" based on "the modulus (M)," but because *Langston* also expressly discloses that the value of "W" must be a power of two in direct contradiction of Claims 7, 38, 50, and 62, the Applicant respectfully submits that, for at least the reasons stated above, Claims 7, 38, 50, and 62 are allowable over the art of record and is in condition for allowance.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Craig G. Holmes
Reg. No. 44,770

Date: April 6, 2005

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop AMENDMENT, P.O. Box 1450, Alexandria, VA 22313-1450.

on 4/6/05 by Tracy Reynolds
Tracy Reynolds